CI Hearing Folder

[redacted]

18 December 1985

To: D/ICS

From: [redacted]

STAT

Subject: SSCI Letter to NSC With Recommendations on the Report by the Information Security Oversight Office

We were given a courtesy copy of the subject SSCI correspondence, which Mr. Garfinkel in effect solicited during his testimony before the SSCI in its hearing on the Stilwell Commission Report last month.

[redacted]

[redacted]

STAT

[redacted]

cc: DD/ICS
EXO/ICS

United States Senate

SELECT COMMITTEE ON INTELLIGENCE
WASHINGTON, DC 20510

#85-4252

December 13, 1985

The Honorable Robert C. McFarlane
Assistant to the President for
National Security Affairs
The White House
Washington, D.C. 20500

Dear Bud:

On November 29, 1985, Mr. Steven Garfinkel, Director of the Information Security Oversight Office, advised the Select Committee that he expected action early next year on the initiatives he has recommended to improve the Government-wide information security system. Mr. Garfinkel discussed these proposals with the Committee at a hearing on November 20 and indicated that the National Security Council would like to have our input on these or other initiatives the Committee might propose.

Attached are the Committee's recommendations on information security in response to Mr. Garfinkel's invitation. We appreciate the opportunity to comment on his proposals, and we are grateful for the excellent cooperation we have received from the Executive branch on all aspects of our review of counterintelligence and security programs. We look forward to continuing to work with the NSC staff on an agenda for immediate action and long-range decisions in this area.

Sincerely,

Dave Durenberger
Chairman

Patrick Leahy
Vice Chairman

Attachment

SENATE SELECT COMMITTEE ON INTELLIGENCE
RECOMMENDATIONS ON INFORMATION SECURITY

The Director of the Information Security Oversight Office (ISOO) has recommended a series of initiatives to improve the Government-wide information security system. They reflect a well-founded concern about five problems: overclassification or unnecessary classification; overdistribution of classified information; inadequate classification management; erosion of the need-to-know principle; and unauthorized disclosure. The ISOO recommendations were developed in consultation with the agencies most involved with national security information, and they parallel several points made by the DoD Security Review Commission. The Select Committee on Intelligence has reviewed the ISOO recommendations and submits the following proposals.

1. <u>Background</u>

The Select Committee has a long-standing interest in the information security system. The Committee provided input to the Administration in 1977 and in 1982 on the succeeding Executive Orders on National Security Information. The Committee's report on "National Security Secrets and the

Administration of Justice" led to enactment of the Classified Information Procedures Act of 1980, which set procedures for minimizing unnecessary disclosure of national security secrets in criminal prosecutions. The Intelligence Identities Protection Act and the CIA Information Act were both enacted with Committee support so as to improve protection of vital intelligence sources and methods. In each instance, the Committee sought to strike a balance between legitimate interests in secrecy and disclosure.

The upsurge in espionage cases during 1984-85 has focused more attention on weaknesses in information security policy. The cases have highlighted the security problems that result, in large measure, from attempting to protect too much and thereby stretching personnel and other security programs too thin. The issue is not just inadequate resources, but attitudes as well, and the concerns date back many years. No one has characterized the situation better than the late Justice Potter Stewart, who wrote in the Pentagon Papers Case in 1972:

> I should suppose that moral, political, and practical considerations would dictate that the very first principle ... would be an insistence upon avoiding secrecy for its own sake. For when everything is classified, then nothing is classified, and the system becomes one to be disregarded by the cynical or the careless, and to be manipulated by those

> intent on self-protection or self-promotion. I should suppose, in short, that the hallmark of a truly effective internal security system would be the maximum possible disclosure, recognizing that secrecy can best be preserved only when credibility is truly maintained.

Concern about failure to meet these standards is widespread in and out of government.

During the past year, the Committee has been undertaking a comprehensive review of counterintelligence and security policies of the United States. This review has included not just highly-publicized espionage cases and other specific security problems, but the full range of counterintelligence efforts and security programs designed to protect sensitive information and activities from hostile intelligence operations. In this context, the Committee has taken a careful look at information security policy and its relationship with other security disciplines (personnel, physical, communications, computer, and technical security) as well as with counterintelligence programs. The Committee's recommendations are being submitted to the Assistant to the President for National Security Affairs as part of continuing consultations between the Committee and the NSC, with the aim of reaching agreement on an agenda for immediate actions and long-range decisions to improve U.S. counterintelligence and security programs.

2. Immediate Implementation

The Committee believes the ISOO recommendations are an excellent agenda for short-term actions to improve the information security system, although as noted below the Committee has several additional proposals for long-range decisions. Other recommendations that require prompt action at the departmental or national level include many of those contained in the Stilwell Commission report, the Inman Panel's classified annex on overseas technical security, and the latest National Assessment of the Hostile Intelligence Services Threat and U.S. Countermeasures. The Committee supports the President's recent action to establish a new interagency committee, chaired by a member of the NSC staff, to ensure effective action on recommendations to control the hostile intelligence presence and to improve security awareness programs. Strong leadership is essential to carry out effectively the recent legislation on controlling travel by Soviet bloc nationals at the UN Secretariat and on equivalence between U.S. and Soviet official representation. The NSC should promptly address other pending counterintelligence and security recommendations, including the ISOO recommendations, and assign responsibilities for implementation.

The ISOO recommendations themselves are carefully drafted to tighten the administration of the current classification system. Even if more fundamental changes are needed, as the Committee believes, they should not be an excuse for delay. Especially important are the revisions proposed in Executive Order 12356 to require the reporting of improper classification, to require agency heads to ensure personal accountability for management of classified information, and to require effective internal oversight and periodic reconfirmation of special access programs.

These revisions, along with the other directives and policy changes recommended by ISOO, should have the strong, publicly-stated endorsement of the President and the principal members of the National Security Council. The Secretaries of State and Defense, the Attorney General, the Director of Central Intelligence, and the Assistant to the President for National Security Affairs should make clear to their subordinates, publicly where appropriate, their commitment to the new information security policies for curbing overclassification and overdistribution, improving classification management, enforcing the need-to-know principle, and improving security awareness and investigations of unauthorized disclosures. They should hold senior executives and program managers personally responsible for effective implementation.

3. National Strategic Security Program

The Committee's review of counterintelligence and security policies in this "year of the spy" has found troublesome evidence of a lack of overall national policy guidance, especially with regard to the security programs and countermeasures that are supposed to protect classified information. The Committee believes there is a need for a comprehensive and integrated National Strategic Security Program to coordinate and foster the protection of information and activities having the greatest strategic importance. This does not mean establishing a counterintelligence "czar" or taking from individual agencies and officials their responsibility for implementing national policies as they affect their work. Rather, the NSC's statutory mandate to advise the President with respect to the integration of domestic, foreign, and military policies relating to the national security gives it the responsibility to ensure coherent national policy direction and implementation for:

- Information security and classification
- Personnel security
- Telecommunications and computer security
- Technical surveillance countermeasures
- Physical security
- Industrial security
- Research and development efforts
- Security awareness requirements.

To assist the NSC, a single body should be assigned responsibility for policy planning and analysis of all aspects of strategic security. In addition, there must be more effective coordination among the various overlapping forums that now share responsibility for security policy, including the DCI's Security Committee, the National Telecommunications and Information Systems Security Committee, and the Interagency Group-Countermeasures.

This is not an entirely new concept. The need for national policy guidance was identified in 1957 by the Commission on Government Security, whose Vice Chairman was Senator John Stennis. It proposed an office to ensure greater uniformity and higher quality for personnel and industrial security throughout the government. Earlier this year, the Chairman and Ranking Minority Member of the Senate Permanent Subcommittee on Investigations, Senators Roth and Nunn (who also serve on the Select Committee), recommended establishment of an executive body with Government-wide personnel security oversight responsibilities similar to those which the ISOO now has for information security.

The DoD Security Review Commission emphasized a similar need within the Defense Department. The Stilwell Commission stressed "that all security disciplines have as their fundamental purpose the protection of classified information and must be applied in a fully balanced and coordinated way." Thus, the Commission urged the Secretary of Defense to consider placing related security policy responsibilities in a single OSD staff element, with the Defense Security Institute having an expanded policy support mission. (The ISOO recommendations call for the DSI to have a Government-wide role in basic training for all Executive branch security personnel.)

The Stilwell Commission's idea makes sense at the national level as well. The NSC should assign to an appropriate body the task of putting together a fully balanced and coordinated National Strategic Security Program for protecting the most sensitive information and activities. A senior official should be designated to testify on the National Strategic Security Program before the appropriate Committees of the Congress.

4. Streamlining the Classification System

The information security system requires more extensive reform than would result from the ISOO initiatives. While they would clearly help, the recommendations are based on the premise that, as Mr. Garfinkel stated to the Committee, the current structure is "fundamentally sound and, for the most part, works quite well." The Committee disagrees.

The Stilwell Commission reported that "too much information appears to be classified and much at higher levels than is warranted." It found that little scrutiny is given to classification decisions "out of ignorance or expedience" and that "few take the time to raise questionable classifications with originators." Like Mr. Garfinkel, however, General Stilwell saw the problems as "primarily a matter of inadequate implementation of existing policy, rather than a matter of deficient policy."

The Committee shares the view of information security experts who see a fundamental, underlying problem in the complexity of the system. There are at least four levels of classification. Overlaying the three levels prescribed by Executive Order -- Confidential, Secret, and Top Secret -- is a complicated set of special access programs developed by various departments and agencies. The proliferation of special access programs is testimony to the failure of the current classification system. Mr. Garfinkel testified that "a number of these programs are probably unnecessary," and the Stilwell Commission reported that some special access programs actually afford less security protection than ordinary classification requirements.

If the classification system is to work in practice, it must be streamlined so that officials better understand their responsibilities. The Committee supports the ISOO and Stilwell Commission recommendations to require, rather than simply permit, challenges to classification believed to be improper. The impact will be limited, however, unless the classification rules are simplified.

The Committee recommends consideration of a two-level system, based essentially on the current Secret-level standard and the Sensitive Compartmented Information (SCI) model used in the Intelligence Community. The Confidential classification should be dropped, as recommended nearly thirty years ago by the Commission on Government Security. In its 1957 report, the Commission observed that the danger of access to Confidential-level information was "not significant" and that the minimal clearance requirements for such access afforded "no real security check."

Whatever the legal formula for classification, the threshold should reflect a policy that classifies information only where truly necessary to maintain national security. As stated recently by General Eugene F. Tighe, former Director of DIA, "[I]f the U.S. security system for handling classified material is to be useful, only data that are critical to the United States' status as a political, economic and military power should be classified." The initial decision should be whether the information requires protection in order to prevent substantial harm to identifiable national security interests. Rather than assuming that information is classified, the burden should be to show the need for secrecy.

The other standard should focus on the much smaller universe of data that requires special protective measures above and beyond the normal safeguards for classified information. As is the case with intelligence data classified

SCI, classification at the second level should be based on a full analysis of the risks of compromise. Such analysis should ensure that special protective measures are imposed only where necessary and are not diluted by applying them too widely. Careful analysis should also provide the elements for more effective security briefings that help senior policy-makers as well as lower level employees understand the consequences of a security breach.

In the long run, simplifying the classification system will give the ISOO recommendations a much greater chance of reversing the natural incentives to overclassification and enforcing the need-to-know principle.

5. <u>Disclosure Procedures</u>

Disclosure of classified information to the news media raises a different set of issues. The Committee is especially concerned about leaks that compromise sensitive intelligence sources and methods. Such leaks will continue unless something is done about the underlying attitudes that foster disrespect for the rules of secrecy.

The Committee endorses the ISOO recommendation that new educational materials, both classified and unclassified, be developed to address the damage caused by unauthorized disclosures. More effective unclassified materials are especially important. The Committee has found the security orientation briefings offered routinely by the Executive branch fall short of minimal requirements, even though some security officials can do an excellent job of explaining the significance of classification and compartmentation policies.

Even more important than education, however, are the procedures for authorized disclosure of classified information to the news media. The ISOO recommendation for reassessment of the policies for leak investigations may accomplish little without adequate controls over authorized disclosures. Currently, the practice of non-attributable background statements, often drawing on classified information, is pervasive. Such statements are virtually indistinguishable from leaks. They divert the overworked investigators of leaks from the cases in which administrative discipline, dismissal, or legal action is possible; and they reinforce the climate of cynicism that leads to leaks and counterleaks.

Senior officials who authorize disclosures of classified information on background, without permitting attribution to the source, gain two advantages that undermine an effective information security system. First, they often can conceal their responsibility for the disclosure, just as the leaker does. Second, they can avoid giving the originating agency a chance to argue against disclosure and explain the harm it would do. If the same information disclosed "on background" were contained in a press release, it would have to be formally declassified. In practice, however, classified information authorized for disclosure on background technically remains classified. There may well be valid reasons for retaining a "background" briefing's classified character; but any serious effort to address the problem of leaks clearly must confront this practice and bring it under control.

Therefore, one of the most important actions to deter leaks and to change the atmosphere that promotes leaks would be to require, by Executive order, that agreed procedures be followed whenever any official authorizes disclosure of classified information to the news media. The procedures should apply not only to formal statements for attribution, but also to disclosures on background. They should require either that the information be declassified or that a record be maintained for purposes of accountability when authority is exercised or granted to disclose to the news media information that remains classified. Such procedures should include the requirements to consult the agency that originated the information and to designate the officials permitted to exercise or grant this authority.

Strong leadership is needed to break through the cycle of leak and counter-leak that pervades the policy community and jeopardizes highly sensitive intelligence sources and methods. The time is ripe to face the realities of press-government relations and adopt sensible rules that bring some order to the chaos that has fostered disrespect for security.

6. Conclusion

The ISOO recommendations can make an important contribution to national security if they are implemented vigorously with high-level support. The Committee believes they should become part of a National Strategic Security Program that is monitored by the NSC and the Congress. They should also lead to more fundamental reforms to simplify the classification system and to establish procedures with consultation and accountability for authorized disclosures. These initiatives, together with actions in other areas of counterintelligence and security that the Committee is considering, can ensure a level of protection for sensitive information and activities commensurate with the threats and vulnerabilities the United States will face in the years ahead.